Doc Code: AP.PRE.REQ

PTO/SB/33 (07-05)
Approved for use through xx/xx/200x. OMB 0651-00xx
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE

PRE-APPEAL BRIEF REQUEST FOR REVIEW

Docket Number (Optional): 061047-0264493

I hereby certify that this correspondence is being deposited with the United States Postal Service with sufficient postage as first class mail in an envelope addressed to "Mail Stop AF, Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450" [37 CFR 1.8(a)]

on _____

Signature _____

Typed or printed name _____

Application Number	Filed
09/870,584	June 1, 2001

First Named Inventor: SUDIA

Art Unit	Examiner
2135	P. Klimach

Applicant requests review of the final rejection in the above-identified application. No amendments are being filed with this request.

This request is being filed with a notice of appeal.

The review is requested for the reason(s) stated on the attached sheet(s).
Note: No more than five (5) pages may be provided.

I am the

- [ ] applicant/inventor.
- [ ] assignee of record of the entire interest. See 37 CFR 3.71. Statement under 37 CFR 3.73(b) is enclosed. (Form PTO/SB/96)
- [X] attorney or agent of record. Registration number 42663.
- [ ] attorney or agent acting under 37 CFR 1.34. Registration number if acting under 37 CFR 1.34 _____

Signature

Jean-Paul G. Hoffman
Typed or printed name

703.770.7794
Telephone number

April 8, 2008
Date

NOTE: Signatures of all the inventors or assignees of record of the entire interest or their representative(s) are required. Submit multiple forms if more than one signature is required, see below*.

[X] *Total of 1 forms are submitted.

Attorney Docket: 061047-0264493
Client Reference: AUTH-II

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re PATENT APPLICATION of: SUDIA *ET AL.* Confirmation Number: 9326

Application No.: 09/870,584 Group Art Unit: 2135

Filed: June 1, 2001 Examiner: P. Klimach

Title: METHOD FOR SECURELY USING DIGITAL SIGNATURES IN A COMMERCIAL CRYPTOGRAPHIC SYSTEM

April 8, 2008

ATTACHMENT SHEETS TO PRE-APPEAL BRIEF CONFERENCE REQUEST

In response to the Final Office Action dated January 8, 2008 ("Action"), Appellant hereby requests for the reasons below that a panel of examiners formally review the legal and factual basis of the rejections in this application prior to the filing of an appeal brief. This request is being filed with a Notice of Appeal.

APPEALED REJECTIONS

Appellant traverses and appeals the rejection of claims 1, 18-21, 72-78 and 116-129 under 35 U.S.C. §112, second paragraph, of claims 1, 21, 72, 73, 77, 78, 116-120, 129 and 130 under 35 U.S.C. §103(a) as being unpatentable in view of U.S. Patent No. 5,745,574 ("Muftic"), U.S. Patent No. 4,953,209 ("Ryder") and U.S. Patent No. 5,852,666 ("Miller"), of claims 18, 20, 74, 121-128 and 131 under 35 U.S.C. §103(a) as being obvious in view of Muftic, Ryder, Miller and U.S. Patent No. 5,940,510 to Curry et al. ("Curry") and of claims 79, 80, 83, 84 and 109-115 under 35 U.S.C. §103(a) as being obvious in view of Muftic, Ryder, Miller and Curry.

ARGUMENTS FOR TRAVERSAL

Rejection under 35 U.S.C. §112

The application as filed clearly discloses examples of, prior to digital signing, denying access to the public key or more generally denying utilization of the public key as claimed. In one example embodiment, the public key is not distributed to the recipient unless the recipient performs the digital signing. See, e.g., Applicant's specification, page 35, lines 24-33. Therefore, the user is denied access to, or more generally denied utilization of, the public key prior to the digital signing is performed. In another example embodiment, a secure device contains the public key but the recipient cannot utilize the public key, i.e., the public key cannot be obtained from the secure device, until the recipient performs the digital signing. See, e.g., claim 18. Again, the user is denied utilization of the public key prior to the digital signing is performed. The Office Action appears to focus on restrictions on the recipient, disclosed in page 36, lines 5-15 of the specification, after the recipient has the public key. However, that doesn't argue against denying access to the public key

in the first place until the recipient has performed the digital signing clearly disclosed in, for example, page 35, lines 24-33.

Rejection under 35 U.S.C. §103(a) in view of Muftic, Ryder and Miller

As acknowledged in the Action, the cited portions of Muftic fail to at least disclose or teach, in response to digital signing of a message by a recipient by which said recipient agrees to rules, permitting said recipient to utilize said public key and prior to said digital signing, denying utilization or use of said public key, as recited in claims 1 and 73.

Applicant submits that the cited portions of Muftic also fail to disclose or teach agreeing to rules including a rule regarding maintaining secrecy of the public key, as recited in claims 1 and 73.

In cited col. 10, lines 52-57, Muftic merely discloses the nature of a certificate from a certifying authority and the process of requesting such a certificate from the certifying authority. Such a certificate in Muftic is requested by forwarding a public key and thus the certificate requestor already has access to or use of a public key. The public key in Muftic is freely available to users. There is no indication or teaching in the cited portions of Muftic of a recipient of a public key maintaining the public key secret, let alone a recipient agreeing to rules including a rule regarding maintaining secrecy of the public key. The Office Action appears to be improperly reading secrecy restrictions in col. 10, lines 52-57 of Muftic. There is simply no use of secrecy or confidential terminology in that cited portion.

Further, even assuming *arguendo* that the cited portions of Ryder are properly combinable with the cited portions of Muftic (which Applicant does not concede and disagrees that they are), Applicant submits that the cited portions of Ryder fail to overcome the shortcomings of the cited portions of Muftic, or vice versa. Ryder merely discloses a system for electronically transmitting data objects such as computer programs with a means for verifying that the computer program was actually received and the terms and conditions of its use accepted by the receiver is presented. (Ryder, Abstract). The cited portions of Ryder simply have no disclosure or teaching regarding a public key. Accordingly, the cited portions of Ryder simply have no disclosure or teaching regarding in response to a digital signing, permitting a recipient to utilize a public key and prior to the digital signing, denying utilization of a public key. The cited portions of Ryder further have no disclosure or teaching regarding rules including a rule regarding maintaining secrecy of the public key, let alone digitally signing a message including the rules, by which said recipient agrees to the rules. Ryder does not even include the words secret or confidential.

Further, even assuming *arguendo* that the cited portions of Miller are properly combinable with the cited portions of Muftic and Ryder (which Applicant does not concede and disagrees that they are), Applicant submits that the cited portions of Miller fail to overcome the shortcomings of

the cited portions of Muftic and Ryder, or vice versa. The cited portions of Miller simply have no disclosure or teaching regarding in response to a digital signing of a message, permitting a recipient to utilize a public key and prior to the digital signing, denying utilization of a public key. Rather, the cited portions of Miller merely disclose an object decrypting a message containing an object reference. For example, there is nothing in the cited portions regarding any digital signing and indeed Miller teaches away by stating at col. 8, lines 58-60 that "[m]ethod (1) is known as signing and is not used by the preferred embodiment."

Further, the cited portions of Miller have no disclosure or teaching regarding a rule regarding maintaining secrecy of a public key, let alone digitally signing a message containing such a rule, by which said recipient agrees to the rule. Rather, those cited portions of Miller merely disclose encrypting the object reference for supply to an intended object so as to prevent outsiders from being able to access the object reference during transmission and to help ensure the intended object receives the message with the object reference. That does not disclose a rule to be agreed by a recipient that a public key is to be maintained in secret. Moreover, those cited portions of Miller do not disclose a message containing such a rule and a recipient digitally signing a message containing such a rule, by which the recipient agrees to such a rule. Rather, the cited portions of Miller merely disclose a message containing an object reference and a location of the referenced object referenced; there is no rule regarding maintaining secrecy of a public key in that message. Moreover, there is no indication in the cited portions of Miller that the intended object digitally signs the message containing such a rule or that the intended object has an obligation to maintain a public key secret.

Rejection under 35 U.S.C. §103 in view of Muftic, Ryder, Miller and Curry

As discussed above, claims 1 and 73 are patentable over the cited portions of Muftic, Ryder and Miller. Further, even assuming *arguendo* that Curry is properly combinable with the cited portions of Muftic, Ryder and Miller (which Applicant does not concede and disagrees that they are), the cited portions of Curry do not overcome the shortcomings of the cited portions of Muftic, Ryder and Miller, or vice versa. Curry merely disclose a secure device that may have the ability to store or create a private/public key set, whereby the private key never leaves the secure device and is not revealed under almost any circumstance. (Curry, col. 4, lines 49-52). Therefore, the cited portions of Curry alone or in combination with the cited portions of Muftic, Ryder and Miller, fail to disclose or render obvious, *inter alia,* in response to digital signing of a message by a recipient by which said recipient agrees to rules, permitting said recipient to utilize said public key and prior to said digital signing, denying utilization or use of said public key, as recited in claims 1 and 73. Only with improper hindsight based on Applicant's disclosure could the Office Action assert that a

public key could be equally kept unrevealed in Curry's secure device, particularly given that Curry recognizes the private key / public key distinction. Curry merely adopts the well-known practice of keeping a private key secure and would not to a person skilled in the art teach or suggest, prior to digital signing of a message by a recipient by which said recipient agrees to rules, denying utilization or use of said public key and in response to said signing, permitting said recipient to utilize said public key.

Moreover, the cited portions of Curry further fail to disclose or teach agreeing to rules including a rule regarding maintaining secrecy of the public key, let alone digital signing of a message by a recipient by which said recipient agrees to such rules, as recited in claims 1 and 73. Curry is simply silent regarding the obligations of a user of Curry's device 108.

Rejection under 35 U.S.C. §103 in view of Muftic, Ryder, Miller and Curry

Even assuming *arguendo* that the cited portions of Muftic, Ryder, Miller and Curry are properly combinable (which Applicant does not concede and disagrees that they are), the cited portions of Muftic, Ryder, Miller and Curry fail to disclose or render obvious a method of enforcing a security policy in a cryptographic system comprising, *inter alia*, providing a recipient with a message containing rules of said system and with a secure device containing an inactive form of said public key, wherein said public key cannot be obtained from said device, and in response to said recipient digitally signing said message, activating said public key in said secure device, as recited in claim 79.

Applicant respectfully submits that the citations to col. 15, lines 32-43 and col. 12, lines 60-64 of Muftic are inapposite to claim 79. In those citations, Muftic merely discloses a certifying authority re-signing a certificate, which involves a certifying authority generating a new key pair for generating the certificate. Those citations fail to provide any disclosure or teaching regarding an inactive form of a public key, let alone about a secure device containing the inactive form of the public key and from which the public key cannot be obtained (except in response to said recipient digitally signing said message, which activates the public key) or about activating the public key.

Further, as discussed above, the cited portions of Ryder simply have no disclosure or teaching regarding a public key. Accordingly, the cited portions of Ryder simply have no disclosure or teaching regarding an inactive form of a public key, let alone about a secure device containing the inactive form of the public key and from which the public key cannot be obtained (except in response to said recipient digitally signing said message, which activates the public key) or about activating the public key.

The cited portions of Miller merely disclose an object decrypting a message containing an object reference. The cited portions of Miller thus simply have no disclosure or teaching regarding

an inactive form of a public key, let alone about a secure device containing the inactive form of the public key and from which the public key cannot be obtained (except in response to said recipient digitally signing said message, which activates the public key) or about activating the public key. There is simply no indication of any public key in Miller having an inactive form. There is simply no indication in Miller of any secure device containing a public key, let alone in inactive form.

Further, Applicant submits that the cited portions of Curry do not overcome the shortcomings of the cited portions of Muftic, Ryder and Miller, or vice versa. As discussed above, the cited portions of Curry simply have no disclosure or teaching regarding an inactive form of a public key, let alone about a secure device containing the inactive form of the public key and from which the public key cannot be obtained (except in response to said recipient digitally signing said message, which activates the public key) or about activating the public key. Only with improper hindsight based on Applicant's disclosure could the Office Action assert that a public key could be equally kept unrevealed in Curry's secure device, particularly given that Curry recognizes the private key / public key distinction. Curry merely adopts the well-known practice of keeping a private key secure and would not to a person skilled in the art teach or suggest a secure device containing an inactive form of a public key and from which the public key cannot be obtained (except in response to said recipient digitally signing said message, which activates the public key) or about activating the public key.

CONCLUSION

The rejected dependent claims are patentable by virtue of their dependency, and for the additional features recited therein. Therefore, it is respectfully requested that the panel return a decision concurring with Appellant's position and eliminating the need to file an appeal brief because there are clear legal and/or factual deficiencies in the appealed rejections.

Respectfully submitted,
PILLSBURY WINTHROP SHAW PITTMAN LLP

JEAN-PAUL G. HOFFMAN
Reg. No. 42663
Tel. No. 703.770.7794
Fax No. 703.770.7901

Date: April 8, 2008
P.O. Box 10500
McLean, VA 22102
703.770.7900